

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT  
EASTERN DIVISION OF OHIO**

<b>In the Matter of the Search of:</b>	)	No.
	)	
<b>The residence located at 803 Colonial Drive,</b>	)	
<b>Heath, Ohio 43056, including any curtilage or</b>	)	
<b>detached buildings, and any computers, related</b>	)	
<b>digital media, or digital devices located therein;</b>	)	<b>Magistrate Judge</b>
<b>the person of Justin S. Kling, any vehicle he is</b>	)	
<b>occupying or that is registered to him and any</b>	)	
<b>computers or digital media located therein/thereon</b>	)	

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

**I. EDUCATION TRAINING AND EXPERIENCE**

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including the online exploitation of children.
2. During my career as a police and task force officer, I have participated in hundreds of investigations regarding computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses and child exploitation. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252(a), 2252A, 2251 and 2422.

3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

## **II. PURPOSE OF THE AFFIDAVIT**

4. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachments A and B** of this 803 Colonial Drive Heath, Ohio 43056 (the SUBJECT PREMISES), the person of Justin S. Kling (the SUBJECT PERSON), a 1999 Dodge Ram bearing Ohio registration JNQ2842 (collectively the SUBJECT VEHICLES), and the content of any computers or other electronic storage devices located in/on the SUBJECT PREMISES, SUBJECT PERSON, and SUBJECT VEHICLES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the production, advertising, distribution, transmission, receipt, and/or possession of child pornography, which items are more specifically described in **Attachment C** of this Affidavit.
5. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of a cell-site search warrant; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the production, advertising, distribution, transmission, receipt, and/or possession of child pornography, are presently located at/on the SUBJECT PREMISES, SUBJECT PERSON, and SUBJECT VEHICLES. I have not omitted any facts that would negate probable cause.

### **III. APPLICABLE STATUTES AND DEFINITIONS**

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. The term “child pornography”<sup>1</sup>, as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.
10. The term “sexually explicit conduct”, as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), “sexually explicit conduct” when used to define the term child pornography, also means “(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.”
11. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
12. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
13. “Graphic” when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).

---

<sup>1</sup> The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as

14. The term “computer”<sup>2</sup> is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
15. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
16. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
17. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
18. As it is used throughout this affidavit and all attachments hereto, the term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

#### **IV. BACKGROUND REGARDING THE INTERNET, DIGITAL STORAGE DEVICES AND MOBILE APPLICATIONS**

19. I know from my training and experience that computer hardware, computer software, and electronic files (“objects”) may be important to criminal investigations in two distinct

---

referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

<sup>2</sup> The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities

ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

20. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
21. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
22. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.
23. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media

---

of these devices differ from that of a traditional computer, they are discussed separately and distinctly.



that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 16 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 64 Gigabytes to 256 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

24. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their

customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses<sup>3</sup> and other information both in computer data format and in written record format.

25. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
26. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
27. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount



of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
29. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment C**.

## **V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the

warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

- 31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

## **VI. INVESTIGATION AND PROBABLE CAUSE**

- 32. On June 17, 2022, law enforcement officers with the Licking County Sherriff's Office (LCSO) received a report indicating that John Doe One, a sixteen-year-old male, was offered money and other gifts in exchange for engaging in sexual acts with an adult male. In conducting an investigation into these allegations, LCSO contacted John Doe One who then participated in a forensic interview on June 27, 2022. During that interview, John Doe One revealed that Matthew Reif (REIF) had shown him adult pornography and pornography involving minor children on multiple occasions over the last two years. More specifically, LCSO learned that John Doe One and the family of John Doe One knew REIF through their association with the Heath Church of Christ located in Heath, Ohio. John Doe One also revealed that REIF asked him for photos of his erect penis. In addition, John Doe One advised that REIF had solicited nude photos of other juvenile males that both he and REIF were acquaintances with. More specifically, John Doe One identified a juvenile

relative of REIF and indicated that REIF's relative had once disclosed to John Doe One that REIF had taken his nude photos in the past.

33. That same day, as a follow-up to the interview with John Doe One, an interview with REIF was conducted by the LCSO. During that interview, REIF admitted to offering John Doe One money and other gifts, including Jordan tennis shoes, in exchange for John Doe One allowing REIF to engage in acts of masturbation with him. REIF further admitted that he had solicited two other male juveniles for photos of their penises and that those images were sent to REIF in exchange for REIF sending the juvenile's money and gifts. REIF noted that these conversations with the juvenile males, including John Doe One, occurred primarily via text message and the mobile application, Snapchat. Furthermore, REIF acknowledged to law enforcement with the LCSO that he utilized the email addresses matt17reif@gmail.com and djlittlemattie@gmail.com.
34. On or about July 1, 2022, REIF was arrested by the LCSO for violations of the Ohio Revised Code (ORC) relating to Pandering Obscenity Involving a Minor (2907.32) and Illegal Use of a Minor in Nude Oriented Material (2907.323).
35. On or about July 6, 2022, search warrants seeking to seize digital media devices belonging to REIF were executed by LCSO. Several digital media devices, including a Puanv USB drive, Micro SD cards, Apple iPad, and an Apple Macbook were recovered pursuant to those warrants.
36. The investigation by LCSO further revealed that REIF was employed as a travelling surgical technician which required him to commute for work. More specifically, law enforcement learned that REIF drove to Indiana for work and commuted back and forth between Ohio and Indiana for his job. In doing so, REIF maintained a residence at 140 Greer Drive in Newark, Ohio on the weekends and during the week, resided at 222 Forest Drive in Jeffersonville, Indiana. On July 5, 2022, an additional search warrant was obtained for REIF's Jeffersonville, Indiana address by the Indiana State Police. As a result of that search warrant, numerous digital media devices were seized to include two digital cameras, an Apple Macbook, Apple iPad, and iPhone, SD cards, and a hard drive.
37. During the seizure processes of the digital media devices belonging to REIF, LCSO began to preliminarily review the potential evidence contained on them. A cursory review of the Puanv USB drive seized from REIF's vehicle revealed numerous file folders, each of which was identified with the name of a male as the file folder title. Contained within

each individual folder were videos which depicted different males, both juvenile and adult, engaged in acts of masturbation. In addition, a number of videos and images saved within the folders appeared to have been created via the Snapchat app.

38. Through further investigation, law enforcement with the LCSO learned that many of the males depicted within these folder files were local to the Newark, Ohio area and began attempting to identify the males based on their name and/or images and/or saved files. Although the investigation is still ongoing at this time, approximately a dozen males who have been identified thus far admitted to distributing photos or videos of themselves nude and/or masturbating via Snapchat when they were between the ages of fourteen and seventeen years of age. Although a majority of these males advised they knew REIF, they all separately believed that they were communicating on Snapchat with a female named Nicole Smith when they distributed image and videos of themselves on Snapchat. LCSO further noted that the Snapchat videos and images recovered from REIF's Punav USB drive depicted Snapchat conversations between a male and a purported female who used a female name and female emoji while communicating. It is believed, based on the investigation thus far, that REIF utilized a female persona on Snapchat to communicate and make contact with the juvenile males, eventually soliciting child sexual abuse material from them, recording that content, and saving it to his USB drive.
39. Further review of two additional SD cards revealed a video of John Doe One masturbating in a shower. LCSO reviewed the video and noted that REIF was in the video and observed placing the camera in the shower. After the camera was placed, John Doe One was depicted entering into the shower and masturbating. After the recovery of this video, John Doe One participated in a second interview, during which, John Doe One admitted that he had gone to a hotel located in Hebron, Ohio with REIF on approximately five to seven occasions when he was fifteen years of age. According to John Doe One, REIF "bribed" him to masturbate in the shower, however, John Doe One stated he was unaware that he was being recorded by REIF at the time.
40. An arrest warrant for REIF was issued by U.S. Magistrate Judge Kimberly A. Jolson on August 12, 2022 pursuant to a criminal complaint for the Sexual Exploitation of a Minor as well as Receipt, Distribution, and Possession of Child Pornography. REIF was then taken into federal custody and arraigned.

41. On September 13, 2022, REIF agreed to a proffer with your affiant and members of the United States Attorney's Office in Columbus, OH. That proffer continued into a second interview that was held with REIF on September 30, 2022 at the Franklin Count Correction Center II. During these conversations with REIF, REIF provided information involving another child exploiter. More specifically, REIF indicated that his personal friend, Justin Kling (KLING), had been involved in the production and receipt of child pornography.
42. Your affiant further learned that REIF and KLING had conversations via text message and Snapchat within the last twelve months, during which, they both discussed their sexual interest in children. REIF confirmed to your affiant that he distributed files of child pornography to KLING at KLING's request via Snapchat and that those images depicted prepubescent males and females. REIF stated that KLING inquired as to how REIF obtained these images but was very cautious about evidence of his child exploitation interests being found on his cellular phone. In addition, REIF indicated that he also sent a Mega<sup>3</sup> link to KLING via Snapchat which contained files of child pornography. REIF recalled that KLING asked how to access the link and REIF explained that he had to download the Mega app to his phone which REIF believes KLING did to access the files.
43. In continuing the conversation regarding their shared interest in child pornography, your affiant learned that REIF asked KLING if KLING had any files of child pornography. In response, KLING sent REIF an image depicting a nude prepubescent female's vagina. KLING asked REIF if he had taken the photo and KLING acknowledged that he had but would not tell REIF who the child was at that time.
44. Your affiant further learned from REIF that KLING had previously resided with a married couple who had three prepubescent daughters living with them inside the residence (herein after VICTIM FAMILY). According to REIF, when KLING verified that he had taken the child pornography image, REIF assumed that the child who was a member of VICTIM FAMILY that KLING had previously resided with in Alexandria, Ohio.
45. According to REIF, KLING eventually stated that KLING took nude photos of at least one of the prepubescent daughters in the VICTIM FAMILY while they were sleeping and had also attempted to digitally penetrate at least one of the girls. Your affiant learned that both

---

<sup>3</sup> Your affiant knows Mega is a cloud storage and file hosting service which allows users to store and share computer files through free accounts.



KLING and REIF were apprehensive about sending child pornography files via Snapchat so when they were together, they would show each other photos on their phones. Your affiant learned from REIF that he believed KLING showed REIF additional images depicting nude images of the children in the VICTIM FAMILY, but REIF could only specifically remember the one described above.

46. REIF advised your affiant that he told KLING about the recorded videos of John Doe One and further shared several of these videos with KLING. According to REIF, KLING was aware of the age of John Doe One in the videos. Prior to showing KLING the videos, REIF asked KLING if he wanted to see them at all and REIF stated that he asked KLING this because KLING was interested in much younger children than REIF was and John Doe One was older than KLING's preferred age.
47. After speaking with REIF, your affiant worked to corroborate any of the information provided by REIF about KLING. Recovered in the forensic extraction of REIF's Apple iPhone 11 was a text conversation between REIF and KLING occurring from approximately September 24, 2021 to October 8, 2021.
48. Your affiant would note that on September 28, 2021 REIF and KLING engaged in a text message conversation, during which, they discussed engaging in sexual intercourse together in conjunction with an eighteen year old female. The following conversation then ensued:

REIF: "Would you fuck a 16 yo lol"  
KLING: "Fuck yeah if I can't get caught"  
REIF: "Haha any younger?"  
KLING: "Maybe depends I guess would u lol"  
REIF: "This all between us?"  
KLING: "Yes"  
KLING: "Of course"  
REIF: "What's the youngest you would fuck"  
KLING: "Maybe 13 or 14"  
REIF: "Damnnn a 13 year old?"  
REIF: "Ok"  
KLING: "Maybe. If she's right for it. Tight Pussy. Hbu"  
KLING: "I ain't no saint bro."  
REIF: "Well between us. Def would fuck 12 or older haha"  
REIF: "Super friggin tight"  
REIF: "This has gotta stay with us tho or we could get in big trouble lol"  
KLING: "No shit"  
REIF: "Lmao. 13 the youngest?"  
KLING: "No I'd probably"  
REIF: "Haha can u imagine if we 3 somed a 12 year old"

REIF: "Insane"  
KLING: **"Savage. Bro fucking savage"**  
REIF: "Would u be down to tear a kid up"  
KLING: **"If some young girl txted and was like let's fuck if he like when and where"**  
REIF: "For sure. What would you take thw mouth or the pussy"  
REIF: "Lol"  
REIF: "Should we text about this kinda stuff on snap so it's not saved on phone records?"  
KLING: **"Both. U got to change it up."**  
REIF: "Haha true true"  
KLING: **"I'm going to delete all this."**  
  
REIF: "Am I the only one I text like this? Haha and me too. We can continue on snap"  
REIF: "U"  
REIF: "Why aren't U texting me back on snap"  
REIF: "Or is it glitched"  
KLING: **"I'm driving"**  
REIF: "Sorry lmao"  
REIF: "Gotta surprise on snap"  
REIF: "U busy?"  
REIF: "Check snap if you're not busy"  
KLING: **"Ok. Give me a minute"**  
REIF: "I kind a like we can talk like this, do you agree?"  
KLING: **"Yes"**  
REIF: "Cool haha I'm free all night"

49. Your affiant then observed a text from REIF to KLING on September 29, 2021 in which REIF "Surprise on snap". On September 30, 2021 the following text conversation continued:

KLING: **"Dude did u delete ur Snapchat? Your is gone from my list"**  
REIF: "It got deleted. Guess I sent u too much stuff"  
KLING: **"What!"**  
REIF: "Yeah. Got an email from Snapchat saying I violated their terms and so my account got deleted"  
KLING: **"Damn"**  
REIF: "Yep"  
REIF: "Oh well maybe it was for the best"  
KLING: **"Didn't u have like 1000 person streaks too"**  
KLING: **"Maybe"**  
REIF: "Well that ended a while ago"  
REIF: "I wanted to get rid of snap anyways"  
REIF: "I'd delete anything U have"  
KLING: **"It got rid of everything I got nothing"**  
REIF: "That's good. I need to as well"

REIF: "It's a good thing it's deleted"

50. During further investigation, law enforcement learned that two separate CyberTipline reports involving REIF were submitted to the National Center for Missing and Exploited Children (NCMEC): CyberTip #103077083 (herein after referred to as CyberTip One) and CyberTip #103317742 (herein after referred to as CyberTip Two).
51. More specifically, law enforcement learned via CyberTip One that, on the evening of September 28, 2021 (EST), two files of suspected child sexual abuse material had been distributed on Snapchat by the Snapchat screen/username "lildudematt". Those two files were both videos, one of which depicted an adult male inserting his penis into the anus of a prepubescent male. The second video file depicted a prepubescent female exposing her vagina and then engaging in acts of masturbation. According to information provided by Snapchat, the email address associated to the "lildudematt" account was noted as matt17reif@gmail.com. In addition to the above information, CyberTip One provided the following information related to the "lilmattitude" Snapchat user:

<b>Date of Birth:</b>	11-01-1995
<b>IP Address:</b>	107.77.235.219
	09/30/21 :20:56 UTC

52. Law enforcement also reviewed CyberTip Two and noted that on the evening of September 29, 2021 (EST), the day after the incident date from CyberTip One, four files of suspected child sexual abuse material had been uploaded to Snapchat by the screen/username "lildudematt". Two of those files were videos, one of which depicted a nude prepubescent female engaged in acts of masturbation. A second video depicted a prepubescent female nude from the waist down. The prepubescent female was observed masturbating. According to information provided by Snapchat for CyberTip Two, the email address associated to the "lildudematt" account was again noted as matt17reif@gmail.com. In addition to the above information, CyberTip Two also provided the same user date of birth and IP address information as noted above in CyberTip One. Your affiant would further note that these two CyberTip reports correspond to the text message exchange between REIF and KLING as noted above.
53. On September 19, 2022, your affiant traveled to the residence of the VICTIM FAMILY and made contact with one of the adult members of the VICTIM FAMILY. Your affiant confirmed that three prepubescent females, between the ages of six years old through

twelve years old, and one prepubescent male resided in the house. Your affiant also learned that KLING had inf act resided with VICTIM FAMILY from approximately 2017 to 2019 and that KLING would babysit the children at times, read them bedtime stories, and put them to bed. Your affiant learned that the adult members of the VICTIM FAMILY were not aware of any inappropriate behavior involving KLING or any of the children and that the VICTIM FAMILY was still friends with KLING and KLING's parents. In addition, your affiant learned that KLING was at the residence of VICTIM FAMILY a few weeks earlier and told VICTIM FAMILY he was residing at 803 Colonial Drive in Heath, Ohio (the SUBJECT PREMISES) with his parents.

54. On September 19, 2022, your affiant traveled to the SUBJECT PREMISES and observed a 2018 Subaru Outback bearing Ohio registration "KLING" in the driveway. A search of the Ohio Law Enforcement Gateway (OHLEG) revealed that the registered owner of that vehicle was the mother of Justin KLING. On September 24, 2022, your affiant traveled back to the SUBJECT PREMISES and observed a 1999 Dodge Ram truck parked in the driveway bearing Ohio registration "JNQ2842." A search of OHLEG revealed that the registered owner is Justin KLING (both vehicles herein after referred to as the SUBJECT VEHICLES).
55. Based on all of the information contained herein, your affiant believes that SUBJECT PERSON, residing at the SUBJECT PREMISES and driving SUBJECT VEHICLES, displays characteristics common to individuals who access online child sexual abuse and exploitation material. Forensic analysis of the digital media devices previously seized per federal search warrants revealed SUBJECT PERSON received and subsequently possessed child pornography. In addition, SUBJECT PERSON made an admission to producing child pornography your affiant confirmed he had access too. Based on the information that had been gathered to date, , your affiant believes that there is probable cause that the digital media devices located thereon the SUBJECT PERSON or therein the SUBJECT RESIDENCE and SUBJECT VEHICLES attributed to Justin KLING contain evidence of Justin KLING's child pornography and child exploitation activities.

## **VII. SEARCH METHODOLOGY TO BE EMPLOYED**

56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of items described in **Attachment**

C found at the SUBJECT PREMISES or in the SUBJECT VEHICLES or on the SUBJECT PERSON consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Specifically, such techniques may include, but are not limited to:

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in **Attachment C**;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in **Attachment C**;
- c. Surveying various files, directories and the individual files they contain;
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment C**; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment C**.

#### **VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN**

57. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

- a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.



- b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of

individuals with whom they have been in contact and who share the same interests in child pornography.

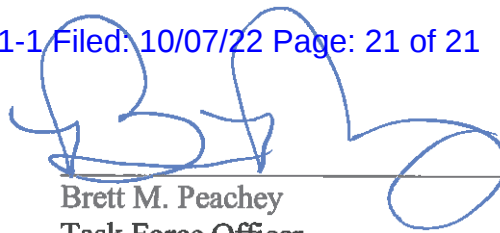
- f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

58. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

59. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution and possession of child pornography is currently located in the SUBJECT PREMISES or SUBJECT VEHICLES or on the SUBJECT PERSON.

## **XI. CONCLUSION**

60. Based on all the forgoing factual information, there is probable cause to believe that of violations of 18 U.S.C. §§ 2251, 2252 and 2252A have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the SUBJECT PREMISES or SUBJECT VEHICLES or on the SUBJECT PERSON listed in **Attachment A and B**, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the SUBJECT PERSON, SUBJECT PREMISES, and SUBJECT VEHICLES described in **Attachment A and B**, and the seizure of the items described in **Attachment C**.



Brett M. Peachey  
Task Force Officer  
Federal Bureau of Investigation

Sworn to and subscribed before me this 7<sup>th</sup> day of October 2022.

  
Kimberly A. Jolson  
United States Magistrate Judge